Procedure Title: **Data Center Access**
Document Number: **110304-P-025**
Revision: **1.1**
Process Owner: **Data Center & Operations Team leader**
Date: **September 23, 2009**

Table of Contents

Date Changed	Revisions	Changed By	Revision #
Original	Baseline	DC&O Team Leader	1.0
April 27, 2012	Remove Reference Documents	BPM and DC&O Team lead	1.1

1. Scope

The Data Center Access Procedure defines a controlled means for granting physical access to DTI data centers. Access to DTI data centers must be restricted to promote the preservation of State of Delaware Information Technology and computing services, ensure security of equipment and personnel, maintain integrity of data, and support the availability of systems.

This procedure regulates access to the William Penn Data Center located in Dover, Delaware and Biggs Data Center located in New Castle, Delaware.

2. Roles and Responsibilities

The following contributors play vital roles in the execution of the Data Center Access procedure.

- Computer Operators (CO)
    1. Enforce physical access restrictions to the data center
    2. Verify the existence of approved change control or open incident tickets
    3. Issue temporary key cards
    4. Ensure temporary key cards are properly checked in / checked out
    5. Computer Operators reside within the data center 24/7/365

- Security Office (SO)
    1. Provide adequate supply of key cards to Operations
    2. Audit key card and door access logs for compliance with DTI policies and procedures

- Service Desk (SD)
    1. Collect information about the problem from the caller
    2. Confirm the need for physical data center access
    3. Open call ticket for co-locate customers
    4. Alert CO when physical data center access is required and person(s) needing access

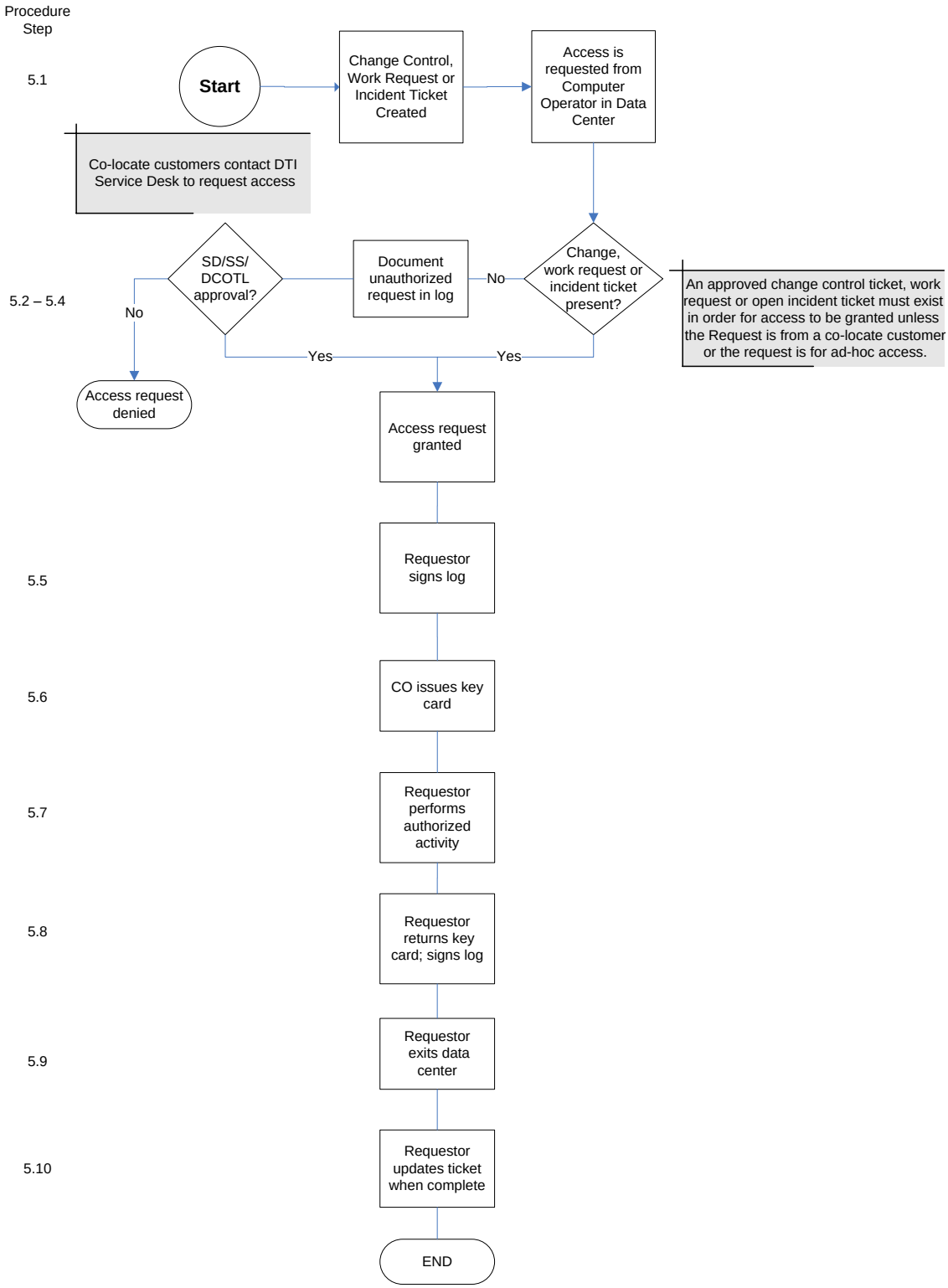
- Site Supervisor (SS)
    1. Provide approval for permanent access to the data center
    2. Provide approval for co-locate customer access to the data center
    3. Provide approval for ad-hoc, impromptu access to the data center
    4. Perform quarterly review of data center access list

- System Control Team ("SCT" consists of System Control Supervisor and Specialist)
    1. Ensure that the Computer Operators receive an automated email from Service Center whenever a change is approved that requires physical access to the data center

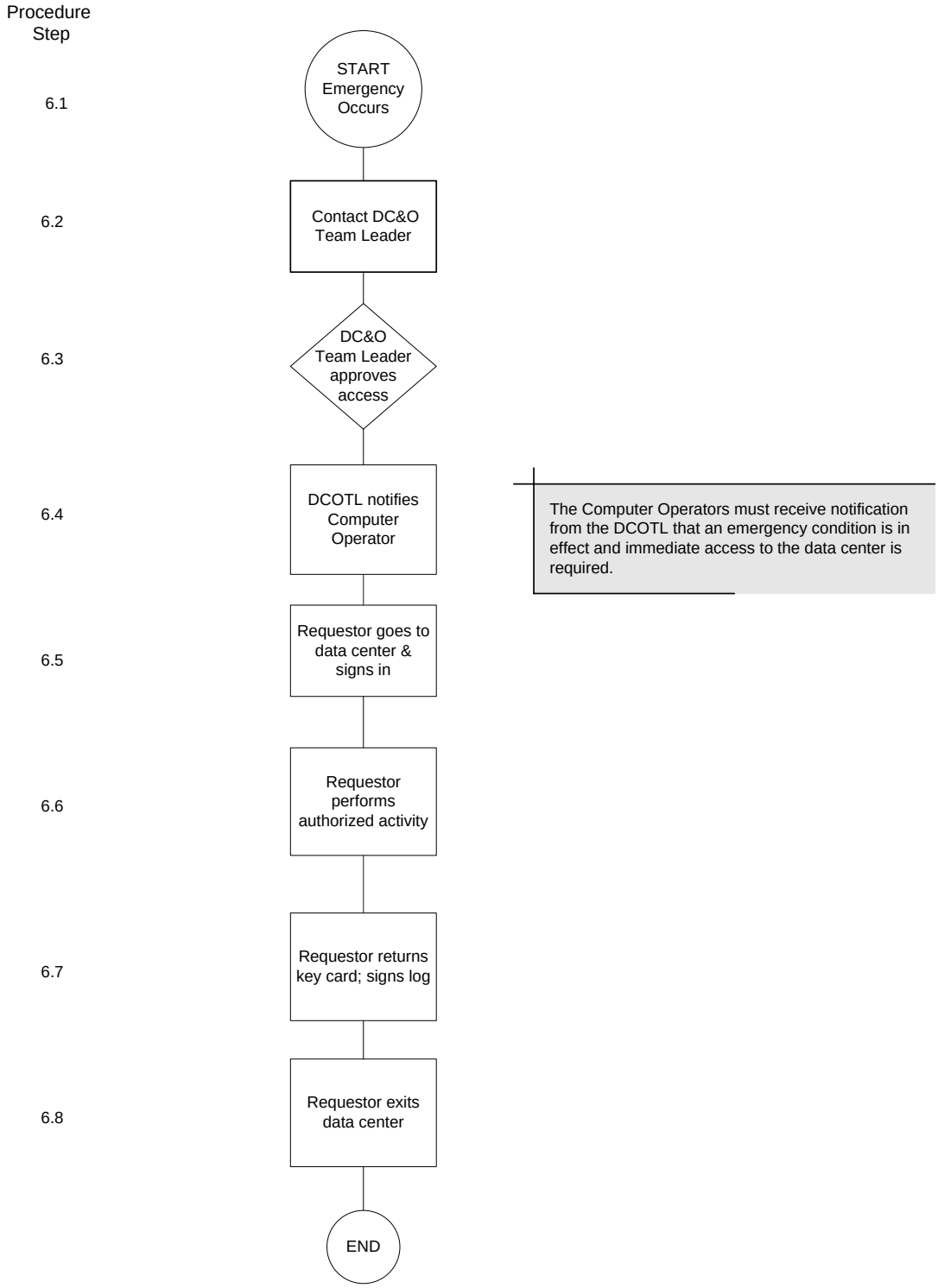
- Data Center and Operations Team Leader (DCOTL)
    1. Approve data center access as the result of an emergency change
    2. Provide CO names of individuals needing emergency access to the data center

- Chief Operating Officer (COO)
    1. Grant approval access to the data center in the absence of the Site Supervisor or the Data Center & Operations Team Leader (DCOTL)

3. Process Flow Diagram: Data Center Access (Regular)



4. Process Flow Diagram: Data Center Access (Emergency)



5. Procedure: Data Center Access (Regular)

Physical access to the Biggs or William Penn data center, for vendors, contractors and state employees requires the existence of an approved change control, work request or open incident management ticket, call ticket, ad-hoc. Entrance and activities performed while in the data center are restricted by the scope of the ticket.

- The System Control Team will ensure that the Computer Operators receive an automated email from Service Center whenever a change is approved that requires physical access to the data center.
- Access for non-DTI Contractors or Vendors requires a ticket to be opened by a DTI employee.
- Co-locate customers should contact the DTI Service Desk to request access to a DTI Data Center.
    - Service Desk staff will call the DTI Site Supervisor or Data Center & Operations Team Leader (DCOTL) to acquire approval.
    - Service Desk staff will note approval of access in call ticket.
    - Service Desk staff will notify requester that access is granted
    - Service Desk staff will notify CO's that requester has approval to access the data center.

Procedure:

5.1. The Requestor goes to the data center and requests access from the Computer Operator (CO).

5.2. The CO ascertains the access reason (i.e. approved change control, work request, incident management ticket, co-locate customer, ad-hoc).

5.3. If the access is for an approved change or a work request, the CO verifies that they have received email notification from Service Center for the individual(s) requesting access. If they have received an email for the requestor, access is granted.

5.4. If the access is for an incident, the CO should have received a call from the Service Desk. The CO may also check for the presence of an open incident ticket or contact the Service Desk for verification.

5.4.1. Note: Normally, no more than two individuals are admitted to resolve a change or incident. Site Supervisor approval must be obtained should more than two individuals seek access per a single request

5.5 If non standard access is granted, the requestor and any additional personnel required to support the activity must sign the access log. The Requestor is responsible for the activities of all others granted access.

5.5.1 Non-standard access includes data center tours, inspections, cleaning and collecting inventory. All non-standard access requires approval and escort determination by the Site Supervisor or DC&O Team Leader.

5.6 The CO issues a temporary key card to the Requestor and records the key card number.

5.7 The Requestor performs the authorized activity.

5.8 The Requestor returns key card to the CO. The CO records the time the card is returned on the access log.

5.9 The Requestor and all additional individuals granted access depart the data center.

5.10 In the event that the incident or approved change was not resolved the requestor may return as long as the ticket is open; re-approval is not required.

5.11 The Requestor is responsible for updating the ticket to indicate that the work is complete.

6. Procedure: Data Center Access (Emergency – Immediate Access Required)

In the event of an emergency, approval to access must be obtained from the Data Center & Operations Team Leader (DCOTL). The DCOTL notifies the Computer Operator (CO) that an emergency condition is in effect and physical access to the data center is needed. Depending on the severity of the crisis, an emergency ticket may be created before or after the issue has been addressed.

Procedure:

6.1 An event has occurred requiring physical access to the data center.

6.2 The DCOTL is contacted and made aware of the situation.

6.3 The DCOTL will determine if the event is an emergency and requires immediate access to the data center.

6.4 If an emergency situation is in effect, the DCOTL will provide the CO with the names of those requiring access to the data center. If not access denied.

6.5 The Requestor goes to the data center, signs in and CO records key card number.

6.6 The Requestor performs the authorized activity.

6.7 The Requestor returns key card to the CO. The Computer Operator records the time the card is returned on the access log.

6.8 The Requestor and all additional individuals granted access depart the data center.

7. Reference Documents

None